UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SHARON MCGEE, individually and on behalf of herself and all others similarly situated, Plaintiff, v. MORTGAGE INDUSTRY ADVISORY CORPORATION Defendant.	Case No. **CLASS ACTION** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Sharon McGee ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against Defendant Mortgage Industry Advisory Corporation ("MIAC" or "Defendant") upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. SUMMARY

1. Plaintiff brings this Action on behalf of herself and all other similarly situated victims as a result of a recent cyberattack and data breach involving the personally identifiable information of current and former customers of Defendant MIAC, a New York company that promotes itself as being the " . . .destination for mortgage industry participants since 1989. MIAC is a unique analytical solutions provider, with the ability to offer a one-stop-shop for whole loan and mortgage risk management solutions, including origination risks, delivery risks, MSR risks, and portfolio risks."[1]

[1] https://miacanalytics.com/about-us/

2. In or about early April, 2023 an unknown and unauthorized criminal actor gained access to MIAC's network and exfiltrated, at a minimum, customer names, social security numbers and other data provided to MIAC ("PII").

3. In Notice of Data Breach letter, attached hereto as Exhibit A, MIAC sent to Plaintiff and Class Members on July 6, 2023, MIAC explains:

> Mortgage Industry Advisory Corporation ("MIAC") is writing to you to notify you of a recent incident that may affect the privacy of some of your personal information. MIAC provides loan valuation and other financial analytics services to mortgage warehouse lenders including Texas Capital Bank ("TCB"), a business partner of Planet Home Lending, LLC ("Planet"). MIAC received your information in connection with providing services to TCB. . .
>
> . . . On April 6, 2023, MIAC became aware of a cyberattack on our systems. We immediately took steps to secure our systems and began an investigation into the nature and scope of the incident. The investigation determined that in connection with the incident there was unauthorized access to certain systems in our environment, and as a result, certain data stored on our systems were subject to unauthorized acquisition on April 6, 2023. We then undertook a comprehensive review of the affected data to confirm what was impacted. The investigation continued through June 8, 2023, to confirm what information related to Planet was impacted so MIAC could begin to obtain address information for affected individuals in order to provide an accurate notice to impacted parties.

4. MIAC further admits in the Notice letter that "[t]he investigation determined that your Social Security number and name were present in the files that were identified as acquired without authorization." MIAC thereafter admonishes victims "MIAC is offering you access to 12 months of complimentary credit monitoring and identity protection services through IDX, a ZeroFox Company, the data breach and recovery expert."

5. To be clear – there are numerous issues with MIAC's Data Breach, but the deficiencies in the Data Breach notification letter exacerbate the circumstances for victims of the Data Breach: (1.) MIAC fails to state whether they were able to contain or end the cybersecurity threat, leaving victims to fear whether the PII that MIAC continues to maintain is secure; (2.)

MIAC's systems were compromised in April of 2023 but they did not notify any victims until three months later on July 6, 2023; (3.) MIAC fails to state how the breach itself occurred; (4.) MIAC admitted in its letter that social security numbers and names were unlawfully acquired yet they leave it up to the victims to ". . . remain vigilant against incident of identity theft and fraud over the next twelve to twenty-four months . . ." All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

6. As a result of the Data Breach, Plaintiff and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their personal information.

7. In addition, Plaintiff's and Class Members' sensitive PII —which was entrusted to Defendant — was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, remains also in the possession of Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to future cyberattacks and theft.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class

Members that their information had been subject to the unauthorized access by an unknown third party.

10. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

11. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant and entities like it, and Defendant was thus on notice that failing to take steps necessary to secure the PII against those risks left that property in a dangerous condition and vulnerable to theft. Defendant was further on notice of the severe consequences that would result to Plaintiff and Class Members from its failure to safeguard their PII.

12. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard customer PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

13. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for months or even years.

14. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

15. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiff and Class Members will incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

19. Plaintiff seeks remedies including, but not limited to, actual damages, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

20. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class.

II. JURISDICTION AND VENUE

21. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interests and costs, there are more than 100 members of the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity – namely, the Plaintiff is an Illinois resident whereas the Defendant is headquartered and incorporated in New York.

22. This Court has personal jurisdiction over Defendant because Defendant is headquartered and does substantial business from and within in this District.

23. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

III. PARTIES

Plaintiff Sharon McGee

24. Plaintiff Sharon McGee is an individual citizen of Illinois and received a Notice of Data Breach letter from Defendant dated July 6, 2023. Plaintiff McGee data was exposed because she had a mortgage with Planet Home Lending, LLC, which was a business partner of Texas Capital Bank. As mentioned in the July 6, 2023 letter, MIAC provided loan valuation and other financial analytics to Texas Capital Bank.

Defendant Mortgage Industry Advisory Corporation

25. Defendant Mortgage Industry Advisory Corporation is a New York company with its principal place of business located in New York City, New York. Defendant provides loan valuation and other financial analytics services to mortgage lenders across the country.

IV. FACTUAL ALLEGATIONS

Defendant's Business

26. According to Defendant MIAC's website:

> For over 30 years, MIAC Analytics has been the preferred destination for sophisticated mortgage industry participants offering transaction execution services, secondary market hedge advisory solutions, third-party mortgage asset valuations, as well as state-of-the-art valuation and risk models incorporating a full range of consumer behavioral risk factors.[2]

27. Defendant collects personally identifiable information from their respective customers in the course of doing business. This personally identifiable information includes the PII which was compromised in the Data Breach alleged herein.

28. Prior to receiving services from Defendant, Plaintiff and Class Members were required to and did in fact turn over their PII.

29. Upon information and belief, Defendant promises to maintain the confidentiality of Plaintiff's and Class Members' Private Information to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiff's and Class Members' Private Information for non-essential purposes.

30. As a condition of receiving Defendant's services, Defendant requires that Plaintiff and Class Members entrust it with highly sensitive personal information.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

32. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members would not have entrusted

[2] https://www.linkedin.com/company/miac/about/ (last accessed June 20, 2023).

Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

33. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Attack and Data Breach

34. On July 6, 2023, Defendant informed Plaintiff and the Class Members via the Notice that:

> On April 6, 2023, MIAC became aware of a cyberattack on our systems. We immediately took steps to secure our systems and began an investigation into the nature and scope of the incident. The investigation determined that in connection with the incident there was unauthorized access to certain systems in our environment, and as a result, certain data stored on our systems were subject to unauthorized acquisition on April 6, 2023. We then undertook a comprehensive review of the affected data to confirm what was impacted. The investigation continued through June 8, 2023, to confirm what information related to Planet was impacted so MIAC could begin to obtain address information for affected individuals in order to provide an accurate notice to impacted parties.

35. The personally identifiable information that was compromised includes, but is not limited to customer names and Social Security numbers and other data provided to MIAC.

36. MIAC further admits in the Notice letter that "[t]he investigation determined that your Social Security number and name were present in the files that were identified as acquired without authorization." MIAC thereafter admonishes victims "MIAC is offering you access to 12 months of complimentary credit monitoring and identity protection services through IDX, a ZeroFox Company, the data breach and recovery expert."

37. To be clear – there are numerous issues with MIAC's Data Breach, but the deficiencies in the Data Breach notification letter exacerbate the circumstances for victims of the Data Breach: (1.) MIAC fails to state whether they were able to contain or end the cybersecurity

threat, leaving victims to fear whether the PII that MIAC continues to maintain is secure; (2.) MIAC's systems were compromised in April of 2023 but they did not notify any victims until three months later on July 6, 2023; (3.) MIAC fails to state how the breach itself occurred; (4.) MIAC admitted in its letter that social security numbers and names were unlawfully acquired yet they leave it up to the victims to ". . . remain vigilant against incident of identity theft and fraud over the next twelve to twenty-four months . . ." All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

38. The Data Breach Notice letter also states that MIAC is offering victims of the Data Breach 12 months of credit monitoring services. With its offer of credit monitoring services, Defendant is acknowledging that Plaintiff and Class Members are subject to an imminent threat of identity theft and financial fraud.

39. Defendant's Notice also acknowledges the present, imminent, and actual threat to Plaintiff and Class Members by enclosing "Steps You Can Take to Help Protect Your Personal Information" and cautions them ". . . remain vigilant against incidents of identity theft and fraud over the next twelve to twenty-four months by reviewing your account statements and immediately report any suspicious activity or incident of suspected identity theft or fraud to your bank or other financial institution(s)." MIAC recognizes the disruption to Plaintiff and Class Members and that through its letter.

40. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

41. Upon information and belief, the PII was not encrypted prior to the data breach.

42. Upon information and belief, the cyberattack was targeted at Defendant as a company that collects and maintains valuable personal and financial data from its many customers, including Plaintiff and Class Members.

43. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and Class Members.

44. Defendant had obligations to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

45. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk

46. It is well known that PII, including Social Security numbers and customer names in particular are invaluable commodities and a frequent target of hackers.

47. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[3]

48. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

49. Individuals are particularly concerned with protecting the privacy of their Social Security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and

[3] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/.

used by hackers. Even if they know their Social Security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

50. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), and, in light of the recent data breaches Wells Fargo has suffered, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

51. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

52. Despite the prevalence of public announcements of data breach and data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

Defendant Had A Duty to Plaintiff and Class Members to Secure Private Information

53. At all relevant times, Defendant had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Defendant became aware that their PII may have been compromised.

54. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class relied on Defendant to secure their PII when they entrusted Defendant with the information required for employment.

55. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

56. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

57. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority."[4] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[5]

58. The ramifications of Defendant's failure to keep its employees' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personally Identifiable Information

59. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[7]

---

[4] 17 C.F.R. § 248.201 (2013).
[5] *Id*.
[6] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed December 10, 2021).
[7] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 10, 2021).

60. As a growing number of federal courts have begun to recognize the loss of value of PII as a viable damages theory, the sale of PII from data breaches, as in the Data Breach alleged herein, is particularly harmful to data breach victims – especially when it takes place on the dark web.

61. The dark net is an unindexed layer of the internet that requires special software or authentication to access.[8] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[9] This prevents dark web marketplaces from being easily identifiable to authorities or those not in the know.

62. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[10] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of

[8] *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/
[9] *Id.*
[10] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web

birth and medical information.[11] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others." [12]

63. Plaintiff and Class Members' PII is a valuable commodity, a market exists for Plaintiff and Class Members' PII (which is why the Data Breach was perpetrated in the first place), and Plaintiff and Class Members' PII is being likely being sold by hackers on the dark web (as that is the *modus operandi* of data thieves) – as a result, Plaintiff and Class Members have lost the value of their PII, which is sufficient to plausibly allege injury arising from a data breach.

64. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[13] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[1415] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[16]

65. The PII stolen in this specific Data Breach was particularly harmful. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

66. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other

---

[11] *Id.*; *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/

[12] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web

[13] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[14] https://datacoup.com/

[15] https://digi.me/what-is-digime/

[16] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Mar. 29, 2021).

> personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

67. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

68. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

69. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19]

70. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with

---

[17] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 10, 2021).

[18] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed December 10, 2021).

[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed December 10, 2021).

other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[20]

71. Given the nature of Defendant's Data Breach, as well as the delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

72. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[21] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers and dates of birth).

73. To date, Defendant has offered its victims *only one year* of identity monitoring services. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

74. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former employees.

Plaintiff's Experience

[20] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

[21] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed December 10, 2021).

75. Plaintiff was required to provide and did provide her PII to Defendant (through Planet Home Lending, LLC) as a condition of receiving services with Defendant.

76. To date, Defendant has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach particularly given the fact that Plaintiff's PII has already been "impacted" in the Data Breach and likely been made available on the dark web to anyone wishing to purchase it.

77. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues when the service number for enrollment does not work properly.

78. Nor has Defendant compensated Plaintiff and Class Members for the time they will spend monitoring their accounts, placing credit freezes and fraud alerts, changing online passwords and other actions that Defendant instructs recipients of the Notice to take.

79. Plaintiff and Class Members have been further damaged by the compromise of their PII in the Data Breach which was "impacted" and is in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII.

80. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

81. Plaintiff stores any documents containing her PII in a safe and secure location, and he diligently chooses unique usernames and passwords for her online accounts.

82. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In

response to the Data Breach, Plaintiff has spent significant time monitoring her accounts and credit score, changing her online account passwords and verifying the legitimacy of the Notice and researching the Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

83. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII — a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach. Defendant acknowledges that Plaintiff and Class Members will need to ". . . remain vigilant against incident of identity theft and fraud over the next twelve to twenty-four months. . ."

84. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

85. Plaintiff suffered emotional distress and increased stress and anxiety as a result of the Data Breach because of the actions he has been forced to undertake, the loss of control over her most intimate information, and the fact that he must remain vigilant for the remainder of her life.

86. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security Number, being placed in the hands of criminals.

87. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff as a condition of sale by Defendant. Plaintiff, however, would not have entrusted her PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

88. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ACTION ALLEGATIONS

89. Plaintiff brings this suit on behalf of herself and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

> All persons Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

90. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

91. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, it is likely that hundreds, if not thousands, of individuals had their PII compromised in this Data Breach, given the Defendant operates in over 100 markets in the United States. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

92. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

i. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

iv. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

v. Whether Defendant owed a duty to Class Members to safeguard their PII;

vi. Whether Defendant breached its duty to Class Members to safeguard their PII;

vii. Whether computer hackers obtained Class Members' PII in the Data Breach;

viii. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

ix. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

x. Whether Defendant's conduct was negligent; and;

xi. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

93. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

94. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

95. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

96. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

97. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

98. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for

certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

xii. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

xiii. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

xiv. Whether Defendant's failure to institute adequate protective security measures amounted to negligence; and

xv. Whether Defendant failed to take commercially reasonable steps to safeguard PII,

99. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE

100. Plaintiff re-alleges and incorporates by reference herein paragraphs 1-100 below.

101. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII for pecuniary gain, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

102. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

103. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. The harm that Plaintiff and Class Members experienced was within the zone of foreseeable harm known to Defendant.

104. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between each Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential PII, a mandatory step in receiving services from Defendant. While this special relationship exists independent from any contract, it is recognized by Defendant's privacy practices, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered PII as part of their businesses and were solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a resulting data breach.

105. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

106. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and the frequency of data breaches in general.

107. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems. It was

foreseeable that Plaintiff and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

108. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

109. Plaintiff and the Class had and have no ability to protect their PII that was in, and remains in, Defendant's possession.

110. Defendant was in a position to effectively protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

111. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

112. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

113. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

115. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

116. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), Defendant had a separate and independent duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

117. The FTCA is intended, in part, to protect individuals whose PII is maintained by another and who are unable to safeguard their information as they cannot exercise control or direction over the data security practices.

118. Plaintiff and the members of the Class are within the class of persons that the FTCA was intended to protect as their PII was collected and maintained by Defendant and they were unable to exercise control over Defendant's data security practices.

119. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

120. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the members of the Class.

121. Defendant breached its duties to Plaintiffs and the members of the Class under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

122. Had Plaintiffs and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiffs and the members of the Class would not have entrusted Defendant with their Private Information.

123. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the members of the Class, they would not have been injured.

125. The injury and harm suffered by Plaintiff and the members of the Class was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiff and the members of the Class to experience the foreseeable harms associated with the exposure of their Private Information.

126. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former employees' PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

127. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

128. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

129. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

130. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
BREACH OF IMPLIED CONTRACT

131. Plaintiff re-alleges and incorporates by reference herein paragraphs 1-100 below.

132. Plaintiff and the Class entrusted their PII to Defendant as a condition of receiving Defendant's services. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen

133. At the time Defendant acquired the PII of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

134. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

135. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

136. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

137. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

138. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

139. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
INVASION OF PRIVACY – INTRUSION UPON SECLUSION

140. Plaintiff re-alleges and incorporates by reference herein paragraphs 1-100 below.

141. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

142. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

143. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party. Defendant's acts and omissions giving rise to the Data Breach were intentional in that the decisions to implement lax security and failure to timely notice Plaintiff and the Class were undertaking willfully and intentionally.

144. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

145. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded and private data.

146. Plaintiff's and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's and Class Members'

PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

147. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

148. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

149. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

150. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT IV
UNJUST ENRICHMENT

151. Plaintiff re-alleges and incorporates by reference herein paragraphs 1-100 below.

152. This Count is brought in the alternative to Count II, Breach of Implied Contract.

153. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiff and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

154. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

155. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

156. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

157. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

158. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

159. Plaintiff and Class Members have no adequate remedy at law.

160. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

161. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

162. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class defined herein, prays for judgment as against Defendant as follows:

a.) For an Order certifying this action as a Class action and appointing Plaintiff and her counsel to represent the Class;

b.) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c.) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Breach;

d.) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e.) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

f.) For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;

g.) For an award of punitive damages, as allowable by law;

h.) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i.) Pre- and post-judgment interest on any amounts awarded and,

j.) All such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury.

DOCUMENT PRESERVATION DEMAND

Plaintiff demands that Defendant take affirmative steps to preserve all records, lists, electronic databases, or other itemization of telephone numbers associated with the communications or transmittal of the calls as alleged herein.

DATED: July 21, 2023

Respectfully submitted,

SHAMIS & GENTILE P.A.
/s/ Andrew Shamis
Andrew J. Shamis, Esq.
New York Bar No. 037343
ashamis@shamisgentile.com
/s/ Christopher Berman
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Tel: (305) 479-2299

EDELSBERG LAW, P.A.
Scott Edelsberg
Florida Bar No. 0100537
scott@edelsberglaw.com
20900 NE 30th Ave., Suite 417
Aventura, FL 33180
Office: (786) 289-9471
Direct: (305) 975-3320
Fax: (786) 623-0915

Counsel for Plaintiff and the Class.

EXHIBIT A

MIAC
MIAC Analytics™
4145 SW Watson Ave
Suite 400
Beaverton, OR 97005

To Enroll, Please Call:
1-888-567-0238
Or Visit:
https://response.idx.us/MIAC
Enrollment Code:
9D5PA4EAR9

Sharon McGee
1S261 Ingersoll Ln
Villa Park, IL 60181-3839

July 6, 2023

NOTICE OF SECURITY INCIDENT

Dear Sharon McGee:

Mortgage Industry Advisory Corporation ("MIAC") is writing to notify you of a recent incident that may affect the privacy of some of your personal information. MIAC provides loan valuation and other financial analytics services to mortgage warehouse lenders including Texas Capital Bank ("TCB"), a business partner of Planet Home Lending, LLC ("Planet"). MIAC received your information in connection with providing services to TCB. MIAC takes the protection of your information very seriously. Although we have no evidence of actual or attempted misuse, identity theft or fraud related to your information as a result of this incident, this letter provides information about the incident, our response, and steps you may wish to take to protect against misuse of your information.

What Happened? On April 6, 2023, MIAC became aware of a cyberattack on our systems. We immediately took steps to secure our systems and began an investigation into the nature and scope of the incident. The investigation determined that in connection with the incident there was unauthorized access to certain systems in our environment, and as a result, certain data stored on our systems were subject to unauthorized acquisition on April 6, 2023. We then undertook a comprehensive review of the affected data to confirm what information was impacted. The investigation continued through June 8, 2023, to confirm what information related to Planet was impacted so MIAC could begin to obtain address information for affected individuals in order to provide an accurate notice to impacted parties.

TCB is Planet's business partner. TCB uses MIAC's financial analytical services. MIAC received Planet customer information in connection with these services. MIAC's investigation revealed that Planet customer information was impacted by the incident. Planet was notified on June 8, 2023, that certain Planet customer non-public personal information was acquired by an unauthorized actor in connection with this incident.

What Information Was Involved? The investigation determined your Social Security number and name were present in the files that were identified as acquired without authorization.

What We Are Doing. We take this incident and the security of information in our care seriously. Upon learning of this incident, MIAC promptly secured its environment, investigated to determine the nature and scope of the incident, and notified law enforcement. MIAC also implemented additional technical safeguards to help prevent a similar incident in the future.

Although we are unaware of any identity theft or fraud resulting from this incident, MIAC is offering you access to 12 months of complimentary credit monitoring and identity protection services through IDX, a ZeroFox Company, the data breach and recovery services expert. Details of this offer and instructions on how to enroll in the services may be found

in the attached *Steps You Can Take to Protect Personal Information*. If you would like to enroll in these services, you will need to follow the attached instructions, as we are unable to enroll you automatically.

What You Can Do. While MIAC is unaware of any actual or attempted misuse of your information as a result of this incident, we encourage you to remain vigilant against incidents of identity theft and fraud over the next twelve to twenty-four months by reviewing your account statements and immediately report any suspicious activity or incidents of suspected identity theft or fraud to your bank or other financial institution(s). You may review the information contained in the attached "Steps You Can Take to Help Protect Your Information." You may also activate your access to IDX identity and credit monitoring services we are making available to you. There is no charge to you for the cost of these services; however, you will need to follow the instructions below to activate your enrollment in this service.

For More Information. If you have questions regarding this incident, you may contact a dedicated assistance line that Planet has set up with MIAC at 1-888 567-0238 between the hours of 9:00am and 9:00pm Eastern. You may also write to MIAC at 521 Fifth Ave., 6th Floor, New York, NY 10175.

Sincerely,

Mortgage Industry Advisory Corporation

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

1. Website and Enrollment. Go to https://response.idx.us/MIAC and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 22, 2023.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-567-0238 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. MIAC recommends consumers periodically obtain their credit reports from each nationwide credit reporting agency and have information relating to any fraudulent transactions deleted. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number or copy of Social Security card;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud and obtain a copy of it. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. MIAC is located at 521 5th Ave., 6th Floor, New Yok, NY 10175.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, you may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. The North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. you may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office the

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 4 Rhode Island residents that may be impacted by this event.